

HOST CERTIFICATION METHOD AND SYSTEM

Lane W. Lee
Timothy R. Feldman
Douglas M. Rayburn
Gary G. Kiwimagi

ABSTRACT OF THE DISCLOSURE

A system and method is provided for authenticating a device. A method includes receiving a certificate from the device, the certificate including a plurality of fields, including a field holding a digital signature from a certifying authority, verifying the digital signatures in the certificate, the verifying including at least one of verifying the certifying authority digital signature using the certifying authority public key; and verifying a device digital signature using a device public key, and receiving validation data from a source, the validation data identifying one or more data in the certificate as valid or invalid according to predetermined criteria, and if the digital signatures are verified and validated, transmitting a session key to the device to establish a secure communication channel.